



IT Systems Engineering | Universität Potsdam

# Firewalling mit iptables

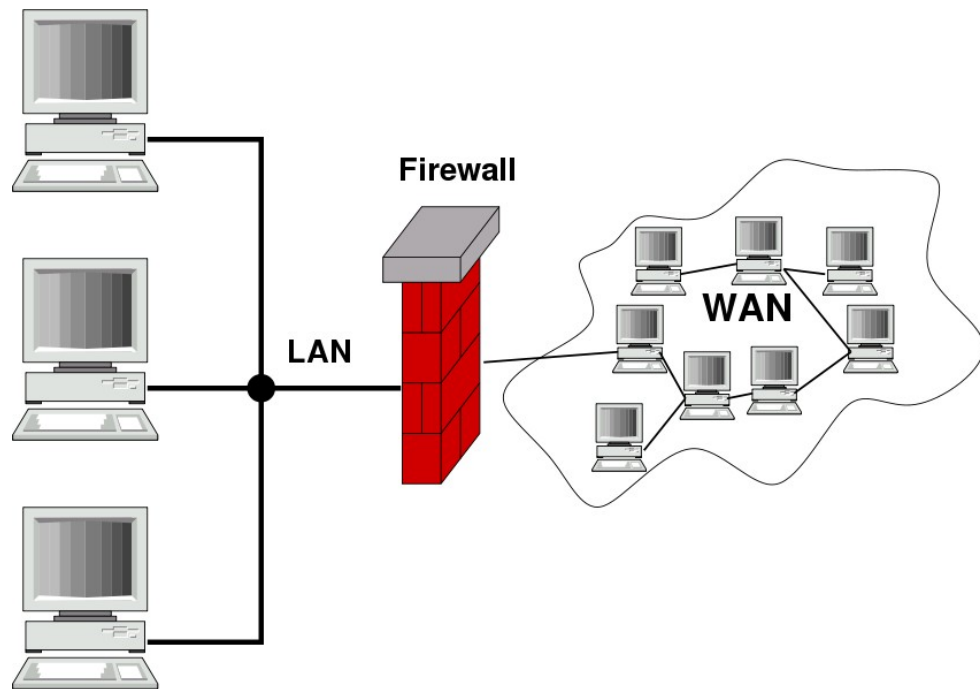
## Die Netfilter-Architektur

Seminar Betriebssystemadministration  
SS 2009

- Firewall
  - Aufgaben/Ziele
  - Firewalltypen
- Sicherheitspolitik
- Sicherheitskonzept
  - Netzwerktopologie
- Iptables
  - Netfilter-Architektur
  - Beispielregeln
  - Konkrete Umsetzung

- Firewall  $\triangleq$  „Brandschutzmauer“
- Trennt zwei Netze
  - Überwachung des Netzwerkverkehrs zwischen diesen Netzen
- Durchsetzen von Sicherheitsbestimmungen (+)
- Protokollierung (+)
- Kontrolliert nur Verbindungen, deren Pakete über sie laufen (-)
- Angriffe von Innen / Untreue Mitarbeiter / Hacker im eigenen Netzwerk (-)

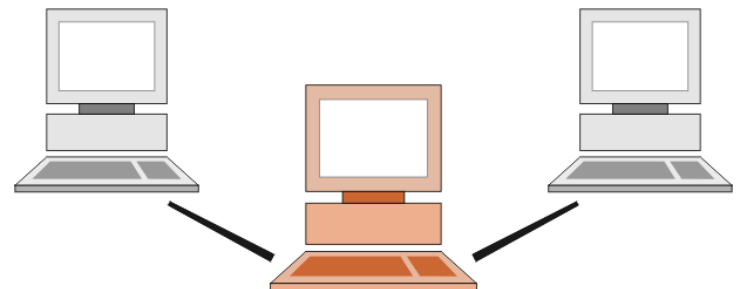
- Firewall
  - besteht aus Soft- (Betriebssystem mit Firewallsystem) und Hardwarekomponenten (Router, Proxy)
- Bridging-Firewall
- Routing-Firewall
- Proxy-Firewall



- Bridge, Switch
- Im Netz nicht sichtbar (+)
- Keine offenen Ports (+)
- Lediglich statische Paketfilterung möglich
- Keine Addressübersetzung (nötig bei Lan ↔ Internet) (-)

- Router
- Filtertechniken auf OSI-Ebene 3 möglich
- Adressübersetzung möglich (NAT)
- Im Netz sichtbar und direkt angreifbar(-)

- Proxy
- Kommunikationspartner zwischen Quell- und Zielsystem (für mindestens eine Seite)
- Zwei eigenständige Verbindungen (!= Routing-Firewall)
- Inhalt der Netzwerkpakete kann zusammenhängend analysiert werden
- Anfragen filtern, Pakete verändern



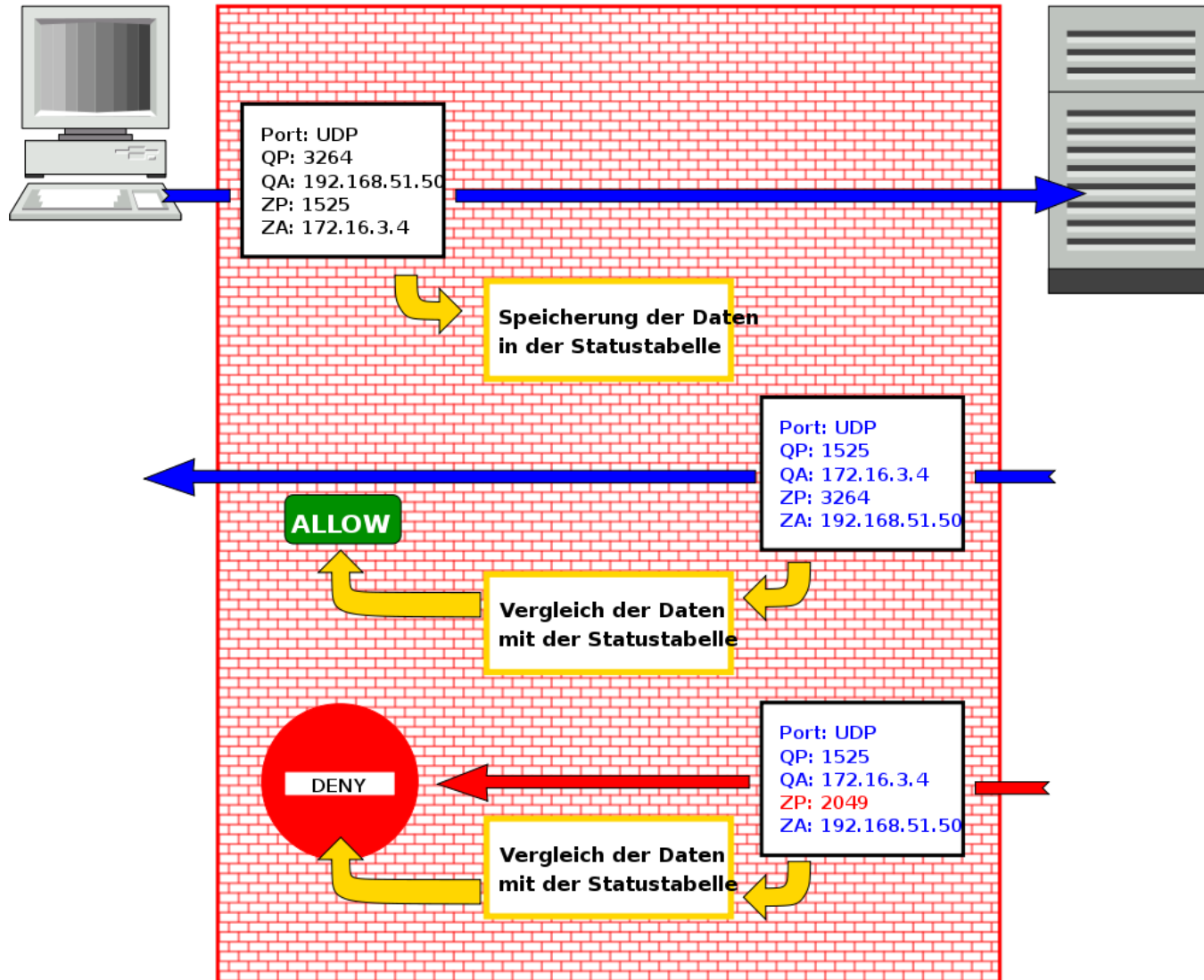
- Paketfilter
- Stateful Packet Inspection
- Application Layer Firewall / Proxy Firewall

- Filterung von Datenpaketen anhand von Quell- und Ziel-Adresse (Ports)
- Definiertes Regelwerk (definierte Regeln vs. Default Regeln)
- Unzulässiges Paket wird verworfen (DROP)
- Paket verwerfen, aber Antwort an Empfänger (REJECT)
- iptables

- Erweiterte, zustandsgesteuerte Paketfilterung (Paketinspektion auf OSI-Schicht 3, 4)
- Statustabelle aller Netzwerkverbindungen
- Zusammenhänge zwischen den Paketen werden erkannt (→ Sitzung)
- Verbindungsaufbau interner Clients und Antworten auf Anfragen der Clients werden erkannt (und können passieren)
- Unangeforderte Daten werden verworfen (trotz bestehender Verbindung)
- Verbindung selbst nicht beeinflusst (!= Proxy)
- iptables

# Stateful Packet Inspection

11



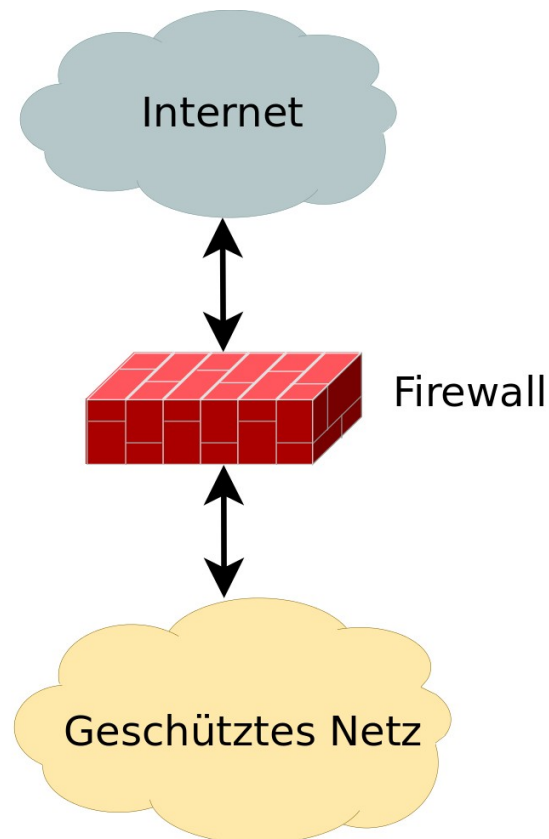
- Beachtet zusätzlich zu den reinen Verkehrsdaten wie Quelle, Ziel und Dienst noch den Inhalt der Netzwerkpakete auf der OSI-Schicht 7
- Ermöglicht dedicated Proxies für höhere Protokolle (Contentfilterung, Malwarescan)

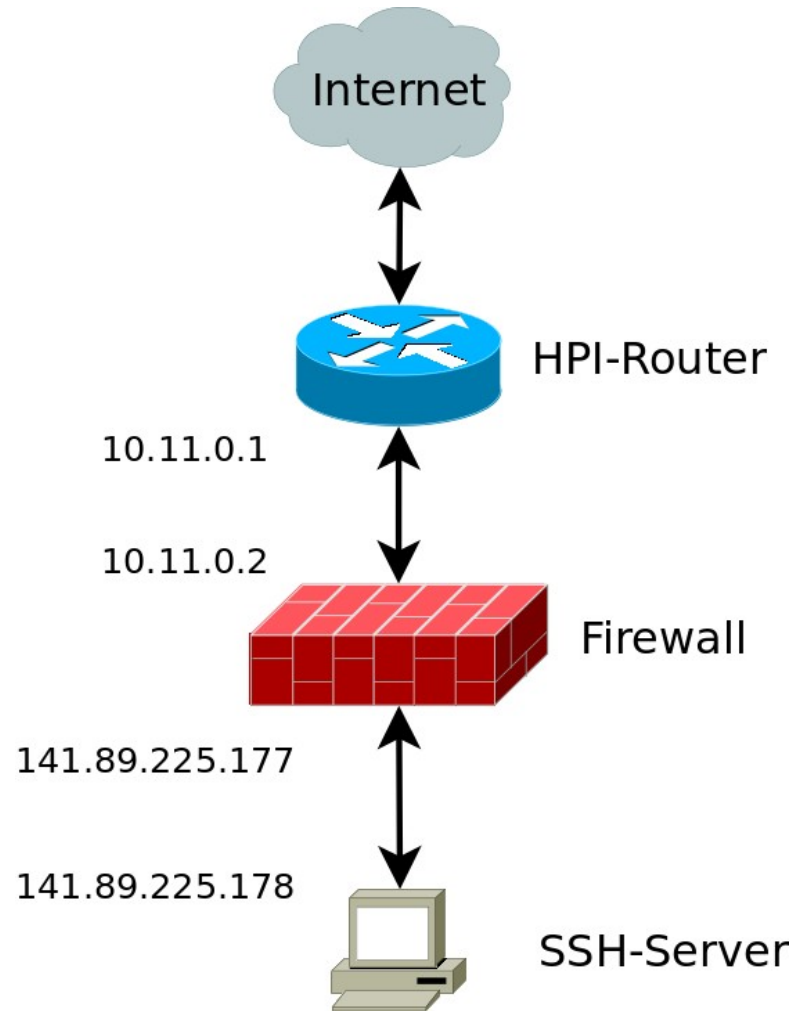
- Entscheidungen des Management
- Absichtserklärung definiert Sicherheitsziele

- Alles, was nicht ausdrücklich erlaubt ist, ist verboten  
(Default Policies)
  - eingehender/weiterzuleitender Verkehr wird standardmäßig blockiert
  - ausgehender Verkehr kann standardmäßig passieren
- Zentraler Schutz der Anwender beim Surfen am Arbeitsplatz
  - zentrale Firewall, die passiert werden muss
- Extern erreichbarer SSH-Server (141.89.225.178)
- Sonstige TCP-Verbindungen müssen aus dem privaten Netz initiiert werden
- Schutz des eigenen Netzwerks nach dem Stand der Technik
  - iptables

- Definition der Verantwortlichkeiten
  - Firewalladmin
- Festlegung von Zugangsberechtigungen, Gruppen, Einzelpersonen
  - Firewallzugang nur durch Admin
- Sicherungskonzepte
  - Logfiles
- Infrastruktur
  - Netzwerktopologie
    - ◇ eine Firewall auf dediziertem Rechner
    - ◇ schützt privates Netz
- IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik, <http://www.bsi.de/>

- Satz globaler IP-Adressen: 141.89.225.176/28



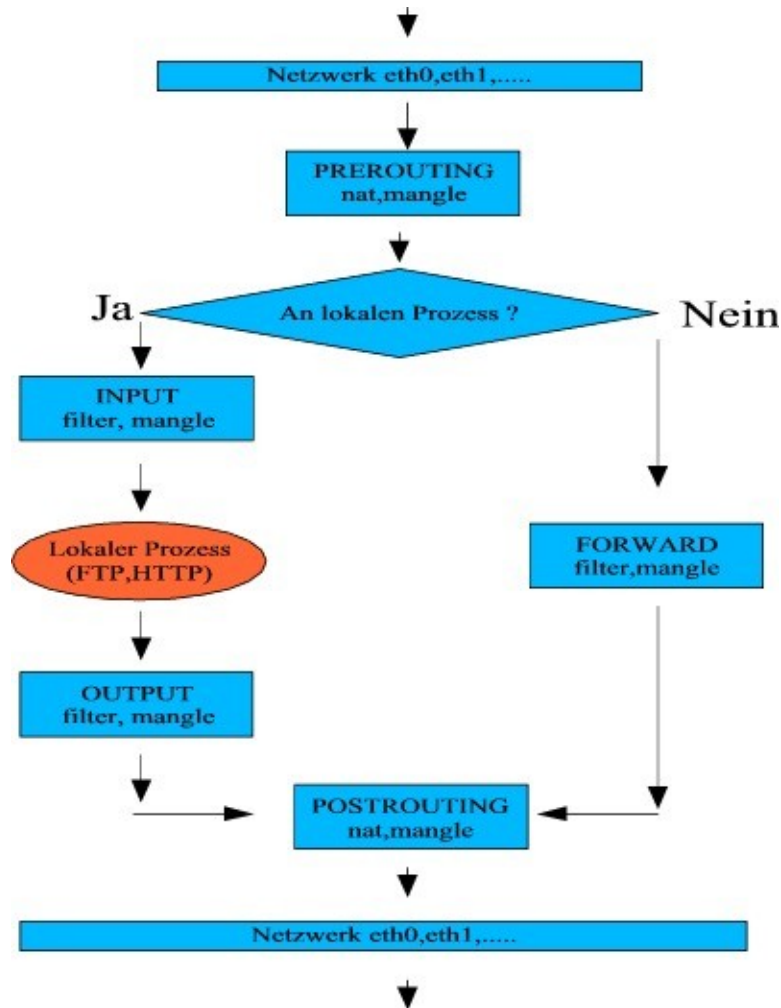


- Netfilter ab Linux-Kernel 2.4: Manipulation von IP-Paketen
- IP Tables: System zum Filtern von IP-Paketen
  - “Nutzer” des Netfilter-Hooksystems
  - Steuerung mittels iptables (user-space)

- Satz von Regeln
- Regeleigenschaften
  - Wann kommt die Regel zur Anwendung
  - Was ist ihre Aufgabe
- Netfilter-Architektur
  - Abbildung auf Chains (wann) und Tables (was)
  - Fünf vordefinierten Chains:
    - ◇ PREROUTING, INPUT, OUTPUT, FORWARD und POSTROUTING
  - Drei vordefinierte Tables:
    - ◇ NAT, MANGLE und FILTER

- Was passiert mit dem Paket?
- NAT (-t NAT)
  - NAT-Regeln ändern die Quell- oder Zieladressen der IP-Pakete (Network Address Translation)
- MANGLE (-t MANGLE)
  - (fast) beliebige Paketmodifikationen
- FILTER (default)
  - Entscheidung ob Paket passieren darf oder verworfen wird

- Lage der Datenpakete bei ihrem Weg durch den Kernel
- INPUT
  - endet beim lokalen Prozess
- OUTPUT
  - beginnt beim lokalen Prozess
- PREROUTING, POSTROUTING und FORWARD
  - Pakete gehen an lokalen Diensten vorbei
  - FORWARD filtert weiterzuleitende Pakete
  
- Filter erlaubt: INPUT, OUTPUT und FORWARD
- Mangle: Alle Chains
- NAT: PREROUTING, POSTROUTING



Um eine Filterregel in einer Chain zu erstellen, verwendet man das Kommando iptables:

*iptables command <chain> <match> -j <ziel>*

## ■ Command

- add (iptables -A)
  - ◇ neue Regel am Ende einer Regelkette
- delete (iptables -D <Regelnummer>)
  - ◇ Löschen einer Regel
- replace ersetzt Regel (iptables -R <Regelnummer>)
- insert fügt Regeln ein (iptables -I <Regelnummer>)
- iptables -L [chain] listet die Regeln einer/aller Chains auf
- iptables -F [chain] löscht alle Einträge einer/aller Regelketten

- Annahme: Regel trifft auf Paket zu („matcht“)
- -j <ziel> gibt an, was mit Paket passieren soll (vordefiniert/benutzerdefinierte Aktion)
- ACCEPT
  - Paket kann passieren
- DROP
  - Paket wird verworfen
- REJECT
  - Paket verschwindet, aber Absender erhält ICMP Fehlermeldung
- Nach einem ACCEPT, DROP oder REJECT ist die Arbeit in einer Chain beendet (Folgeregeln werden ignoriert)

- `<match>` entscheidet ob Regel anzuwenden ist
  - `-s` (source) Quelladresse/-netz
  - `-d` (destination) Zieladresse/-netz
    - iptables -A INPUT -s 192.168.1.0/24 -j DROP*
  - Protokollspezifikation (`-p`)
    - ◇ `-p tcp`, `-p udp` oder `-p icmp`
    - ◇ TCP- und UDP-Ports (-bereiche)
      - `--sport` (source port) und `--dport` (destination port)
      - iptables -A INPUT -p tcp --dport 1:1023 -j DROP*
  - Negation (!)
    - iptables -A INPUT -d ! 192.168.1.0/24 -j DROP*
  - Netzwerkadapterwahl (`-i`, `-o`)

- Match-Module testen auf spezielle Eigenschaften von Netzwerkpaketen (nicht nur Standardparameter)
- Auswahl mittels *iptables -m*
- Optionenanzeige mittels *iptables -m <modul> -h*

- Stateful Filtering/Inspection
  - `-m state <state>`
  - Erlaubt Verbindungen nach ihrem Zustand zu filtern
  - Prüfung ob TCP-, UDP- und ICMP-Pakete zu bestehender „Verbindung“ gehören
  - Analyse von Sequenznummern und Flags in den Paketheadern
  - Verbindungsparameter werden in eigenen Tabellen verwaltet

- <state>
  - NEW
    - Alle Pakete, die eine neue Verbindung aufbauen
  - ESTABLISHED
    - Pakete einer bestehenden Verbindung (Daten von beiden Seiten ausgetauscht)
    - auch für UDP- und ICMP-Pakete (immer verbindungslos)
  - RELATED
    - alles, was logisch zu einer Verbindung gehört, aber kein echter Teil der Verbindung ist
    - z.B. ICMP-Fehlermeldungen einer nicht zu Stande gekommenen Verbindung
    - z.B. aktive FTP-Datenübertragungen, die als separate Verbindungen vom ftp-Server aufgebaut werden, aber logisch zu einer bestehenden Verbindung gehören

## ■ INVALID

- Pakete gehören weder zu einer bestehenden Verbindung, noch zum Versuch, eine neue Verbindung aufzubauen.

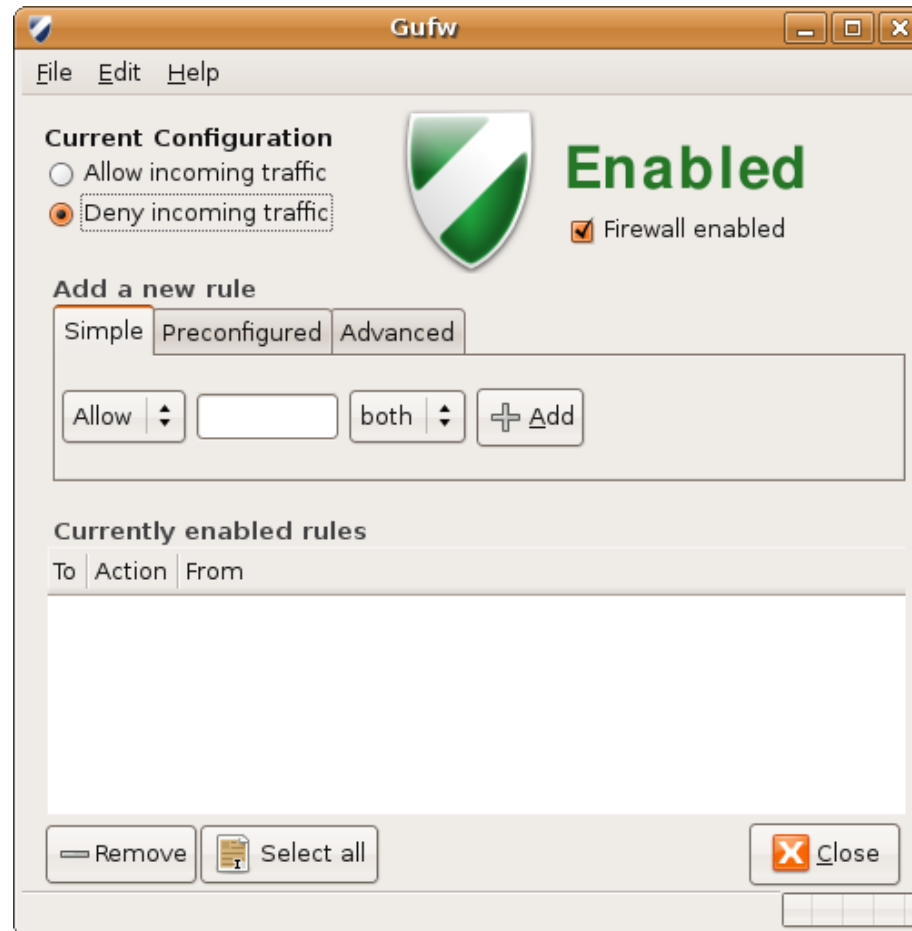
```
iptables -A FORWARD -m state --state NEW -i eth0 -j ACCEPT
```

```
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```



31

- Firestarter
- Gufw



- „Das Firewall Buch“, Wolfgang Barth – Suse Press, 2001
- <http://iptables-tutorial.frozentux.net/iptables-tutorial.html>
- <http://wiki.ubuntuusers.de/iptables2>
- [http://www.pro-linux.de/t\\_netzwerk/iptables.html](http://www.pro-linux.de/t_netzwerk/iptables.html)
- <http://www.pro-linux.de/work/firewall>
- <http://www.heise.de/security/Besser-Filtern-mit-IP-Tables--/artikel/38220/>
- <http://en.wikipedia.org/wiki/Firewall>
- <http://de.wikipedia.org/wiki/Firewall> - Stand 22:25 Uhr 07.07.2009
- [http://en.wikipedia.org/wiki/File:Schematic\\_Proxy\\_Server.png](http://en.wikipedia.org/wiki/File:Schematic_Proxy_Server.png)
- [http://upload.wikimedia.org/wikipedia/commons/d/dc/Stateful\\_inspection\\_udp.svg](http://upload.wikimedia.org/wikipedia/commons/d/dc/Stateful_inspection_udp.svg)
- [http://en.wikipedia.org/wiki/File:GUI\\_for\\_Uncomplicated\\_Firewall.png](http://en.wikipedia.org/wiki/File:GUI_for_Uncomplicated_Firewall.png)